

- ☒ A check in the amount of \$802.00 is enclosed.  
The Commissioner is hereby authorized to charge any other fees which may be required or credit any overpayment to Conley, Rose, & Tayon, P.C., Deposit Account No. 03-2769/5181-60700/BNK.
2. ☒ Specification  
22 page(s) of specification; 6 page(s) of claims, 1 page(s) of abstract
3. ☒ Drawings  
Formal Figure(s) 1-10 on 11 sheet(s)
4. ☒ Oath or Declaration  
☒ Newly executed  
☐ Copy from a prior application (see 37 C.F.R. § 1.63(d))  
Deletion of Inventor(s) (in continuation or divisional applications):  
☐ Delete the following inventor(s) named in the prior non-provisional application:  
  
                      
☐ The inventor(s) to be deleted are set forth on a signed sheet attached hereto.
5. ☐ The entire disclosure of the prior application referred to above is considered to be part of the accompanying application and is hereby incorporated by reference herein.

6. ☐ Microfiche Computer Program (Appendix)
7. ☐ Nucleotide and/or Amino Acid Sequence Submission (if applicable, all necessary)
- ☐ Computer Readable copy
- ☐ Paper Copy (identical to computer copy)
- ☐ Statement verifying identity of above copies
8. ☒ Assignment Papers
9. Power of Attorney
- ☒ Is attached.
- ☐ The power of attorney appears in the original papers of the prior application.
- ☐ Since the power does not appear in the original papers, a copy of the power in the prior application is enclosed.
10. ☐ Information Disclosure Statement (IDS)
- ☐ Copies of IDS Citations
11. Amendments
- ☐ A preliminary amendment is enclosed.
- ☐ Cancel in this application claim(s) \_\_\_\_\_ before calculating the filing fee. At least one independent claim is retained for filing purposes.
- ☐ Amend the specification by inserting before the first line the sentence: \_\_\_\_\_.
12. ☒ Return Receipt Postcard
13. Small Entity Status
- ☐ A small entity statement is enclosed.
- ☐ A small entity statement was filed in the prior non-provisional application and such status is still proper and desired.
- ☐ Is no longer claimed.
14. ☐ Priority of foreign application number \_\_\_\_\_, filed on \_\_\_\_\_ in \_\_\_\_\_ is claimed under 35 U.S.C. §§ 119(a)-(d)
15. ☐ Petition under 37 C.F.R. § 136 for Extension of Time
16. ☐ Other: \_\_\_\_\_

Address all future correspondence to:

B. Noël Kivlin  
Conley, Rose, & Tayon, P.C.  
P.O. Box 398  
Austin, Texas 78767  
Phone: (512) 476-1400 Fax: (512) 703-1250

Signature

Name

Registration No.

Date

B. Noël Kivlin

33,929

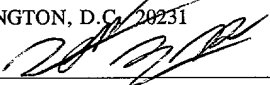
8-7-00

**PATENT**  
**5181-60700**  
**P3917**

"EXPRESS MAIL" MAILING LABEL  
NUMBER EL588940145US

DATE OF DEPOSIT August 7, 2000

I HEREBY CERTIFY THAT THIS PAPER OR  
FEE IS BEING DEPOSITED WITH THE  
UNITED STATES POSTAL SERVICE  
"EXPRESS MAIL POST OFFICE TO  
ADDRESSEE" SERVICE UNDER 37 C.F.R. §  
1.10 ON THE DATE INDICATED ABOVE  
AND IS ADDRESSED TO THE ASSISTANT  
COMMISSIONER FOR PATENTS,  
WASHINGTON, D.C. 20231

  
Derrick Brown

System and Method for Testing Server Latencies  
Using Multiple Concurrent Users in a Computer System

By:

Mark C. Terranova  
Michael P. Shea  
Robert E. Walsh  
Michael V. Iarrobino  
Michael J. Stokes

004080 "SHEA" 004080

## **BACKGROUND OF THE INVENTION**

### **1. Field of the Invention**

5           This invention relates generally to the field of computer systems and, more particularly, to testing server latencies in computer systems.

### **2. Description of the Related Art**

10           Computer systems may include multiple clients coupled to a server. A server may be configured to store information such that the information may be accessed by multiple users using one of the clients. A server may operate using an operating system such as Solaris, Linux, Windows 2000, or Windows NT. An operating system may be configured to create users that may access files on the server. These users may be given varying access privileges to  
15 information on the server and may be included in a group where each member of the group may be given a predefined set of access privileges within the system.

As computer systems become more powerful, servers and their operating systems may become able to support increasing numbers of users in a given system. As the number of users in  
20 the system increases, the number of tasks that the server may need to perform may also increase. The tasks of a server or more particularly, the operating system operating on the server, may include creating and deleting users, logging in and logging out users, performing accesses to files on the server on behalf of users, and possibly executing applications or other programs on the server. As the number of users and hence, the number of tasks increases, the latency in  
25 performing a given task may increase as the task may not be completed until busy resources within the server become available. It would be desirable to measure server latencies in a system with multiple users. It would further be desirable to measure server latencies in a system with

multiple users where the users are modeled according to an organization profile. A system and method to broadly measure server latencies is needed.

## SUMMARY

5

The problems outlined above may in large part be solved by the use of the system and method described herein. Generally speaking, a system and method for testing server latencies using multiple concurrent users in a computer system is provided. A computer system may include a server and one or more clients. Multiple users may be created in the system such that  
10 each user may login to the server. The server may include a directory for each user and the directory for each user may be populated with a mix of files according to a user type for each user. An instance of a test program may be executed for each user on one or more clients concurrently. The server may authenticate each user using the same or different operating system protocols. Each instance of the test program may be configured to cause a series of  
15 accesses to one or more files in the directory of its respective user on the server and may be configured to cause a latency value to be measured and stored for each access that is performed. The latency values may be compiled by each instance of the test program and may be stored onto the server upon completion of each instance of the test program. The latency values measured by an instance of the test program may represent a first time portion that corresponds to the amount  
20 of time to perform a given access and a second time portion that corresponds to the server verifying that the user corresponding to this instance of the test program has permission to access the file. The accesses performed may include read accesses or write accesses.

In one embodiment, a setup program may be configured to create multiple users on a  
25 server in a computer system. The setup program may also be configured to create home directories for each user on the server and may further be configured to populate the home directory of each user with a mix of files that corresponds to the user type of each user. Once the setup program completes, a test script may be initiated. The test script may be configured to

coordinate the concurrent execution of instances of a test program for a set of users in the system. The test script may cause each client in the system to be reset, may cause a system clock to be synchronized, may cause a directory share to be created, and may cause an instance of a test program to be initiated for each of a set of users. Each instance of a test program may generate and store values that may be analyzed in accordance with the type of test being performed.

In one embodiment, a test program may be configured to generate and store latency values associated with accesses to files on the server in the system. A server may authenticate a user corresponding to the test program and may provide a token that may be used by the test program to access files on the server. The test program may cause files within the directory structure of the user to be enumerated into a table and may cause an order of these files to be generated according to a seed value using a random number generator. The test program may then cause read and write accesses to the files in the order generated by the random number generator. The test program may store a latency value associated with each access. Each successive access may be made to the same file as a previous access or to a different file as the previous access. When a file is first accessed, it may be opened on the server and the server may verify that the user associated with the test program has permission to perform an access to the file using the token. The time taken by the server to perform the verification may be reflected in the latency value stored by the test program.

### **BRIEF DESCRIPTION OF THE DRAWINGS**

Other objects and advantages of the invention will become apparent upon reading the following detailed description and upon reference to the accompanying drawings in which:

Fig. 1 is a block diagram illustrating one embodiment of a computer system configured to test server latencies using multiple concurrent users.

Fig. 2 is a flow chart illustrating a method for testing server latencies using multiple concurrent users.

Fig. 3 is a flow chart illustrating a method for setting up a test environment.

Fig. 4a is a diagram illustrating a directory structure.

Fig. 4b is a diagram illustrating one example of populating a directory structure.

Fig. 5 is a table illustrating attributes of different user types for an example organization.

Fig. 6 is a diagram illustrating an example of populating the directory structures of multiple users.

Fig. 7 is a flow chart illustrating a method for concurrently executing instances of a test program.

Fig. 8a is a flow chart illustrating a method for initiating instances of a test program.

Fig. 8b is a first portion of a flow chart illustrating a method for testing server latencies.

Fig. 8c is a second portion of a flow chart illustrating a method for testing server latencies.

Fig. 9a is a table illustrating an example of a directory enumeration table.

Fig. 9b is a table illustrating an example ordering of a directory enumeration table using a first seed value.

Fig. 9c is a table illustrating an example ordering of a directory enumeration table using a second seed value.

Fig. 10 is a block diagram illustrating one embodiment of permission checking structures that may be used by an operation system.

While the invention is susceptible to various modifications and alternative forms, specific embodiments thereof are shown by way of example in the drawings and will herein be described in detail. It should be understood, however, that the drawings and detailed description thereto are not intended to limit the invention to the particular form disclosed, but on the contrary, the intention is to cover all modifications, equivalents, and alternatives falling within the spirit and scope of the present invention as defined by the appended claims.

#### **DETAILED DESCRIPTION OF AN EMBODIMENT**

Turning now to Fig. 1, a block diagram illustrating one embodiment of a computer system configured to test server latencies using multiple concurrent users is shown. Fig. 1 depicts server 100 coupled to clients 120a, 120b, and 120c through network 110. Clients 120a, 120b, and 120c may be configured to execute system processes 122a, 122b, and 122c, respectively. System processes 122a, 122b, and 122c may include operating system routines or other applications. Clients 120a, 120b, and 120c may also be configured to concurrently execute user0 test program 124a through user(m) test program 124(m), user(m+1) test program 124(m+1) through user(n) test program 124(n), and user(n+1) test program 124(n+1), respectively.

Clients 120a, 120b, and 120c are shown by way of example as other embodiments may include other numbers of clients coupled to server 100. Clients 120a, 120b, and 120c may also be configured to execute other types of programs. Clients 120a, 120b, and 120c may be referred



to individually as a client 120 or collectively as clients 120. User0 test program 124a through user(n+1) test program 124(n+1) may be referred to individually as a test program 124 or collectively as test programs 124. Each test program 124 may also be referred to as an instance.

5            Fig. 1 illustrates a system for testing server latencies using multiple concurrent users. Clients 120 may each be configured to concurrently execute one or more instances of a test program 124 on behalf of multiple users. Each user may be created on server 100 such that server 100 may login a user in response to that user attempting to access a file or other resource on server 100. Server 100 may create a home directory for each user and the home directory for  
10    each user may be populated with a mix of files according to a user type for each user as described in more detail below. Each test program 124 may cause communications to take place with server 100 across network 110.

            Server 100 may authenticate a user for each test program 124 using the same or different  
15    operating system protocols. In one embodiment, each instance of test program 124 may be configured to cause a series of accesses to one or more files in the directory of its respective user on server 100 and may be configured to cause a latency value to be measured and stored for each access that is performed. The latency values may be compiled by each instance of test program 124 and may be stored onto server 100 upon completion of each instance of test program 124.  
20    The latency values measured by an instance of test program 124 may represent a first time portion that corresponds to the amount of time to perform a given access and a second time portion that corresponds to server 100 verifying that the user corresponding to this instance of the test program has permission to access the file. The accesses performed may include read accesses or write accesses.

25            Fig. 2 illustrates a method for testing server latencies using multiple concurrent users is shown. Variations on the method are possible and contemplated. Test setup actions may be performed as indicated in block 202. Example test setup actions may include creating users,

creating home directories for the users, and populating the home directories with files according to a user type of each user. Test programs may be concurrently executed using multiple users as indicated in block 204. A test program may, for example, measure and store latencies associated with file accesses. One embodiment of a test program is described below with respect to Figs. 8b and 8c. Test results generated by the test program may be stored as indicated in block 206 and the test results may be synthesized and analyzed as indicated in block 208.

Turning now to Fig. 3, a flow chart illustrating a method for setting up a test environment is shown. Variations on the method are possible and contemplated. Operating system attributes may be set as indicated in block 302. The attributes set may depend on the type of operating system employed by a server such as server 100 shown in Fig. 1.

In one embodiment where a server employs the Windows NT operating system, certain Advanced User Rights may be set to allow a user to impersonate another user. Under normal circumstances, Windows NT may prevent a user from impersonating another user for security reasons. This security enforcement may be overcome by setting the following Advanced User Rights.

1. Act as part of the Operating System
2. Create a Token
3. Increase quotas
4. Replace a process-level token

Once these Advanced User Rights are set, a server may support multiple users from a single client such as clients 120 shown in Fig. 1. A client 120 may use a token to launch multiple instances of test program 124 for different users. Client 120 may do so by copying the token and including impersonate bits in the new token when launching an instance of test program 124. In

doing so, each instance of test program 124 may be effectively executed by a different user and server 100 may interact with each instance as though it were being executed by a different user.

Referring back to Fig. 3, users and user profiles may be created as indicated in block 304 and a home directory may be created for each user as indicated in block 306. Users and corresponding user profiles may be created according to a user creation protocol of an operating system employed by a server. In one embodiment where a server employs the Windows NT operating system, users may be created using the Security Accounts Manager (SAM) database of the Primary Domain Controller (PDC) in a Windows NT domain. In addition, the access control list (ACL) for the home directory of each user may be set.

In one particular embodiment, users may be created using a CreateUsers program. The CreateUsers program may be executed on a client such as client 120 shown in Fig. 1. The CreateUsers program may be used to create a specified number of users and may be executed using the following variables.

Variable	Explanation
MINUSER	First user number
MAXUSER	Number of users to create
HOMEDIR	Location of home directory on server for all users created
HOMECOMPUTER	Location of server (PDC) for all users created
USER PREFIX	Prefix added to user number to create user name
USER POSTFIX	Postfix added to user number to create user name

For example, the following would create user1 to user500 in the current domain.

```
set MINUSER=1
set MAXUSERS=500
```

set HOMEDIR=c:\export\home\users  
set HOMECOMPUTER=venom  
set USERPREFIX=user  
set USERPOSTFIX=  
createusers

In this example, all users would be configured with \\venom\c\$\export\home\users as the directory where their individual home directories would be created. The home directories would be named user0, user1, user2, ..., user 499.

The CreateUsers program may use a MakeUsr program to create users and create a profile for each user. The syntax of the MakeUsr program may be:

makeusr user\_name [password] [switches]

The switches for the MakeUsr program may include:

Switch	Explanation
/DOMAIN	Create a global user account in the domain versus a local user account on the local computer. (Default: local computer).
/LOCAL:local_group	Add account to the specified local_group. Multiple /LOCAL switches may be allowed. In addition, a list of groups may be supplied in the MULOCAL command shell variable.
/GLOBAL:global_group	Add account to the specified global_group. Multiple /GLOBAL switches may be allows. In

addition, a list of groups may be supplied in the MUGLOBAL command shell variable.

	/FULLNAME:name	Specify full name for the account. Use quotes if the name contains spaces.
5	/PROFILEPATH:path	Profile path for this account.
	/SCRIPTPATH:path	Logon script path for this account.
	/HOMEDIR:path	User home directory. If /HOMECOMPUTER is not specified, this may be a local path. If /HOMECOMPUTER is specified, this is a local path relative to that computer (e.g. C: refers to C: on that computer).
10	/HOMECOMPUTER:name	Computer to contain home directory. (Default: local computer).
	/HOMEPROTO:uncpath	Unified naming convention (UNC) name of the prototype home directory. May be copied to the home directory when created.
15	/COMMENT:text	Text comment for this user name

Additional options may be set up by initializing command shell variables prior to executing the MakeUsr program.

A CleanUser program may be used to remove users from the SAM database of a PDC. The CleanUser program may use the following variables.

25	<b>Variable</b>	<b>Explanation</b>
	MINUSER	First user number
	MAXUSER	Last user number
	USER PREFIX	Prefix added to user number to create user name

USER POSTFIX      Postfix added to user number to create user name

For example, the following would delete user100 to user200 in the current domain.

```
5      set MINUSER=100
      set MAXUSERS=200
      set USERPREFIX=user
      set USERPOSTFIX=
      cleanuser
```

10            Fig. 4a is a diagram illustrating generally the creation of a home directory for each user. As may be seen, home directories \user0 and \user1 through \user(n) where n represents the (n-1)th user may be created in a directory named \users. The directory \users may be created anywhere within the directory structure of a server. In Fig. 4a, the root directory of a server may be named \\server and the dashed lines indicate paths to other directories within the directory structure. The directory \users may be directly under the root directory \\server or any number of directories may be included between the root directory \\server and the directory \users.

20            Referring back to Fig. 3, each home directory may be populated according to a user type as indicated in block 308. The home directory of each user may be populated with a set of files that corresponds to a user type for that user. A test program may be configured to perform accesses to these files. Fig. 4b illustrates one example of a home directory populated with files and a directory structure. Fig. 4b shows the directory of user(n), \user(n), populated with files f1, f2, f3, f4, f5, and f6 using directories \d1, \d2, \d3, \d4, \d5, and \d6 as shown. The size of each file f1 through f6 may vary according to a user type for user(n). In addition, the directory structure, i.e. the arrangement of directories \d1 through \d6, may vary according to a user type for user(n). Other home directories may be populated with other numbers and sizes of files as well as other directory structures.

By populating the home directory of a user according to a user type, the concurrent execution of an instance of a test program by multiple users may simulate a user load of an organization on a server. Organizations may comprise different types and number of users that access different sizes and types of files on a server. In order to simulate the user load of an organization, the number and type of users of the organization may be created. Instances of a test program may cause accesses to files in each user's home directory on the server according to a user's user type to simulate a user load of the organization on a server.

Fig. 5 is a table illustrating attributes of different user types of an example organization. Fig. 5 depicts users, file uses, file sizes, load rates, stress rates, and file load mixes for each user type. As shown in Fig. 5, the example organization may include three user types: small, medium, and large. The file uses and sizes indicate the use and size of files typically accessed by each user type. The load rate indicates a network transfer rate for each user type under typical conditions. The stress rate indicates a network transfer rate for each user type under stressed, i.e. test, conditions. The file load mix indicates the percentage of each of three respective files sizes: small, medium, and large. The small file size may refer to files that are 1-2 kilobytes, the medium file size may refer to files that are 20-80 kilobytes, and the large file size may refer to files that are 0.5 to 2 megabytes.

Users in the organization that correspond to the small user type, "small users", may be clerks such as sales assistants, inventory and stock clerks, and accounting clerks. The typical files accessed on a server by small users may be transaction records that are 1-2 kilobytes in size. Small users may have a load rate of 1 megabyte per hour and a stress rate of 6.7 megabytes per hour. Small users may access small files 70% of the time, medium files 20% of the time, and large files 10% of the time.

Users in the organization that correspond to the medium user type, "medium users", may be managers, secretarial workers, and administrative workers. Administrative workers may include human resource representatives, marketing personnel, and executives. The typical files accessed on a server by medium users may be memos and letters that are 20-80 kilobytes in size.

5 Medium users may have a load rate of 1.5 megabytes per hour and a stress rate of 10 megabytes per hour. Medium users may access small files 10% of the time, medium files 70% of the time, and large files 20% of the time.

Users in the organization that correspond to the large user type, "large users", may be technical and creative workers such as engineers, programmers, graphic and mechanical designers, and architects. The typical files accessed on a server by large users may be design files that are 0.5 to 2 megabytes in size. Large users may have a load rate of 1 megabyte per hour and a stress rate of 6.7 megabytes per hour. Large users may access small files 10% of the time, medium files 20% of the time, and large files 70% of the time.

Although the percentage of read accesses versus write accesses may be set by a test program, the default percentage may be set to 80% read accesses and 20% write accesses for each of the user types shown in Fig. 5.

It may be seen that an organization may be readily modeled using the above user types. For example, if the organization is an equipment supplier that designs, markets, and sells its own products, the personnel and the correspond user of types may be modeled as follows.

<u>Department</u>	<u>Title</u>	<u>Number</u>	<u>User Type</u>
Executive	President	1	Medium
	Vice-President	1	Medium
	Secretarial	1	Medium
Sales	Manager/Supervisor	1	Medium





$$\text{Small : Medium : Large} = 24 : 28 : 8 = 3 : 3.5 : 1$$

This ratio represents the mix of small, medium, and large user types that may be presented to a server under test. This user mix may provide a distribution of file accesses that is representative of an actual system such as the system shown in Fig. 1.

Turning now to Fig. 6, a diagram illustrating an example of populating the directory structures of multiple users is shown. As shown in Fig. 6, user home directories \user0, \user1, and \user2 may be created in a directory named \users. The directory \users may be created anywhere within the directory structure of a server. In Fig. 6, the root directory of a server may be named \\server and the dashed lines indicate paths to other directories within the directory structure. The directory \users may be directly under the root directory \\server or any number of directories may be included between the root directory \\server and the directory \users. Similarly, the directory \filemix may be directly under the root directory \\server or any number of directories may be included between the root directory \\server and the directory \filemix.

The directory \filemix may include the directories \small, \medium, and \large. The directory \small may include directory structure 602, the directory \medium may include directory structure 604, and the directory \large may include directory structure 606. Each directory structure 602, 604, and 606 may include a set of subdirectories and files. Directory structures 602, 604, and 606 may each correspond to a different user type. For example, directory structure 602 under the directory \small may correspond to a small user type such as the small user described above in Fig. 5. Similarly, directory structure 604 under the directory \medium may correspond to a medium user type such as the medium user described above in Fig. 5, and directory structure 606 under the directory \large may correspond to a large user type such as the large user described above in Fig. 5. Thus, directory structures 602, 604, and 606 may include a mixture of files and directories appropriate for their respective user types.

Fig. 6 illustrates a method of populating the home directories of a plurality of users. In the example of Fig. 6, user0 may correspond to a large user type, user1 may correspond to a small user type, and user2 may correspond to a medium user type. In order to populate the home directories for each of these users, the directory structure corresponding to each user's user type may be copied from the appropriate directory under the directory \filemix. As illustrated by arrow 616 in Fig. 6, directory structure 606 may be copied to the directory \user0 to populate the home directory of user0. Similarly, directory structure 602 may be copied to the directory \user1 to populate the home directory of user1 as illustrated by arrow 612, and directory structure 604 may be copied to the directory \user2 to populate the home directory of user2 as illustrated by arrow 614.

The method of populating a user's home directory shown in Fig. 6 illustrates one example of how a user's home directory may be populated. Numerous other methods are possible and contemplated. These other methods may include copying directory structures from a wider variety of user types that may have different file mixes than those described, generating directory structures for user types dynamically, or other methods that make files on a server available to a given user.

Turning now to Fig. 7, a flow chart illustrating a method for concurrently executing instances of a test program is shown. A test script may perform the method described in Fig. 7. Client systems may be reset as indicated in block 702. The clocks of the client systems may be synchronized as indicated in block 704. A directory share may be created as indicated in block 706. A directory share may be used to indicate a directory location of the home directories of the users. For example, a directory share "m:" may be created to refer to the directory \users shown in Fig. 6. A test program may be initiated for each user concurrently as indicated in block 708. Test results from each instance of the test program may be stored as indicated in block 710.

002020-9242296-000700

A flow chart illustrating a method for initiating instances of a test program as indicated in block 708 is shown in Fig. 8a. An instance of a test program may be launched for a user as indicated in block 802. A determination may be made as to whether an instance of the test program is to be launched for another user as indicated in block 804. If an instance of the test program is to be launched for another user, then the function performed in block 802 may be repeated.

Turning now to Figs. 8b and 8c, a flow chart illustrating a method for testing server latencies is shown. Each instance of the test program referred to in Fig. 7 may be configured to perform the method described in Figs. 8b and 8c. A user authentication may be performed according to an operating system protocol as indicated in block 806. A user may be logged in to a server using an operating system protocol of a client. The operating system protocols may include a UNIX desktop login method, Windows NT 4.0 Workstation login method, or Windows 2000 Professional login method. The server may validate the logon of the user. An access token may be received as indicated in block 807. The access token may be generated by the server and may be conveyed to the client that is executing the instance of the test program.

Directory enumeration of the files in the user's directory may be performed as indicated in block 808. Figs. 9a, 9b, and 9c illustrate an example of a directory enumeration table and examples of ordering a directory enumeration table using seed values. Figs. 9a, 9b, and 9c refer back to the directory structure shown in Fig. 4b. Directory enumeration table 900 lists the files in the user's directory structure using the directory share created in block 706 of Fig. 7. As may be seen, file 901 may be listed in directory enumeration table 900 as m:\d1\d3\fl. Files 902 through 906 may be listed similarly.

A file order may be randomized using a seed for a random number generator as indicated in block 810. In Fig. 9b, an ordering 910 of directory enumeration table 900 may be created using seed value n shown in seed 912. The seed value n of may be used by a random number

generator to create ordering 910 such that the random number generator may create the same ordering 910 of files 901 through 906 each time the seed value n is used. The order created by using seed value n in Fig. 9b is file 905, file 903, file 904, file 902, file 901, and file 906. Fig. 9c illustrates ordering 920 where seed value n+1, shown in seed 922, may be used. As may be seen, the order created by using seed value n+1 in Fig. 9c, file 904, file 902, file 906, file 905, file 903, and file 901, differs from that created by using seed value n in Fig. 9b.

The test program may be configured to access files (described below with respect to blocks 818 and 820) in the order created by the functions of blocks 808 and 810. In this manner, the results of a test program may be replicated by using the same seed value.

Blocks 812 and 814 indicate waiting for a start time to arrive before proceeding to block 816. The use of a start time may allow the access performed by each instance of the test program to begin concurrently. The chart of Fig. 8b may continue in Fig. 8c as indicated by the circled A.

A file open may be authorized using the access token as indicated in block 816. Fig. 10 illustrates one embodiment of permission checking structures that may be used by an operation system to authorize the opening of a file. Fig. 10 depicts file 1010 with its corresponding file access control list (ACL) 1000. File ACL 1000 may point to data structure 1020 that lists the permissions of each user to file 1010. As may be seen, user0 has read permission as shown in entry 1022, user1 has read and write permission as shown in entry 1024, user2 has no permissions as shown in entry 1026, and user(n) has write permission as shown in entry 1028. When a user's access token is presented to the server where the user seeks to access file 1010, the server may reference file ACL 1000 to determine whether that user has permission to access file 1010.

Once the file open has been authorized, a file may be opened as indicated in block 818. A read or write access may be performed as indicated in block 820. The latency to perform the

read or write access may be measured as indicated in block 822. The latency measurement may include the time to perform the file access as well as the time to authorize the opening of the file. The latency and access information may be stored as indicated in block 824.

5 A determination may be made as to whether the test is complete as indicated in block 826. If the test is not complete, a determination may be made as to whether a new file will be used for a next access as indicated in block 828. If a new file will be used for a next access, then the current file may be closed as indicated in block 830 and the operation may continue at block 816 as indicated. If a new file will not be used for a next access, then the operation may continue  
10 at block 820 as indicated. If the test is determined to be complete at block 826, then results may be stored into a file as indicated in block 832. The results may be stored onto the server.

In one particular embodiment of a test program, the test program may attempt to transfer a specified amount of data within a specified amount of time. If the amount of data to be  
15 transferred is too great to be transferred during the time limit, then the test program may continue until all of the data is transferred. The amount of data to be read or written may be expressed as a ratio, where 1 is read only and 0 is write only. Thus, a ratio of 0.5 along with an amount of data to be transferred of 1 megabyte would indicate that the test program is to read 0.5 megabytes and write 0.5 megabytes.

20 Each instance of test program may not operate continuously. Rather, each instance may be configured to start up at regular, specifiable intervals to perform a part of the total workload. This allows breaks between user activity. For example, the break between activities could be 1, 10, or 60 seconds.

25 The test program may employ the follow parameters.

<u>Parameter</u>	<u>Explanation</u>
------------------	--------------------



Each instance of the test program may save its results in a separate file on the client in which it operates. The results may include the following fields for each access performed.

Field	Description
Field 1	Descriptor for operation (e.g. read or write)
Field 2	Time taken to transfer the data in milliseconds
Field 3	Number of bytes read or written
Field 4	Record size
Field 5	Data and time stamp of operation

The results may further include a summary line with the following fields.

Field	Description
Field 1	Summary descriptor
Field 2	Total read time for test in seconds
Field 3	Total bytes read during the test
Field 4	Bytes read per second
Field 5	Total number of files read
Field 6	Total write time for test in seconds
Field 7	Total bytes written during the test
Field 8	Bytes written per second
Field 9	Total number of files written

The results may be analyzed to determine how a server performed under a user load generated by the test program.

Although the embodiments above have been described in considerable detail, other versions are possible. Numerous variations and modifications will become apparent to those



skilled in the art once the above disclosure is fully appreciated. It is intended that the following claims be interpreted to embrace all such variations and modifications.

002020 "344330

**WE CLAIM:**

1. A system comprising:

a server;

a first client coupled to said server;

wherein said server is configured to login a first user and a second user, wherein said first client is configured to execute a first instance of a test program by said first user and a second instance of said test program by said second user substantially concurrently, wherein said first instance of said test program is configured to cause a first access to a first file on said server, wherein said second instance of said test program is configured to cause a second access to a second file on said server, wherein said first client is configured to store a first latency value associated with said first access, and wherein said second client is configured to store a second latency value associated with said second access.

2. The system of claim 1, wherein said server is configured to verify that said first user has permission to access said first file in response to said first access.

3. The system of claim 2, wherein said first latency value represents a first time portion corresponding to said first access and a second time portion corresponding to said server verifying said first user has permission to access said first file.

4. The system of claim 1, wherein said first user corresponds to a first user type, and wherein said second user corresponds to a second user type.

5. The system of claim 4, wherein server is configured to create a first directory for said first user, wherein said server is configured to populate said first directory with a first plurality of files according to said first user type, wherein said first plurality of files includes said first file, wherein server is configured to create a second directory for said second user, wherein said  
5 server is configured to populate said second directory with a second plurality of files according to said second user type, and wherein said second plurality of files includes said second file.

6. The system of claim 5, wherein said first instance of said test program is configured to identify each of said first plurality of files in said first directory, wherein said first instance of  
10 said test program is configured to create a first order of said first plurality of files using a first seed value, wherein said second instance of said test program is configured to identify each of said second plurality of files in said second directory, and wherein said second instance of said test program is configured to create a second order of said second plurality of files using a second seed value.

7. The system of claim 1, further comprising:

a second client coupled to said server;

20 wherein said server is configured to login a third user, wherein said second client is configured to execute a third instance of said test program by said third user substantially concurrently with initiating said first instance and said second instance, wherein said third instance of said test program is configured to cause a third access to a third file on said server, and wherein said second client is  
25 configured to store a third latency value associated with said third access.

8. The system of claim 7, wherein said server is configured to verify that said third user has permission to access said third file.

9. The system of claim 8, wherein said third latency value represents a first time portion corresponding to said third access and a second time portion corresponding to said server verifying said third user has permission to access said third file.

5

10. The system of claim 1, wherein said server is configured to login said first user using a first operating system protocol, and wherein said server is configured to login said second user using a second operating system protocol.

10 11. The system of claim 1, wherein said server is configured to convey a first token to said first client in response to logging in said first user, and wherein said server is configured to convey a second token to said first client in response to logging in said second user.

12. The system of claim 11, wherein said server is configured to verify that said first user has permission to access said first file in response to said first access using said first token, and wherein said server is configured to verify that said second user has permission to access said second file in response to said second access using said second token.

13. The system of claim 1, wherein said first instance of said test program is configured to cause a third access to a third file on said server, wherein said second instance of said test program is configured to cause a fourth access to a fourth file on said server, wherein said first client is configured to store a third latency value associated with said third access, and wherein said second client is configured to store a fourth latency value associated with said fourth access.

14. The system of claim 1, wherein said first access comprises a first read access or a first write access, and wherein said second access comprises a second read access or a second write access.

15. A method comprising:

logging in a first user to a server;

5 logging in a second user to said server;

executing a first instance of a test program by said first user including:

performing a first access to a first file on said server; and

10 storing a first latency value associated with said first access; and

executing a second instance of said test program by said second user substantially  
concurrently with said executing said first instance of said test program including:

15 performing a second access to a second file on said server; and

storing a second latency value associated with said second access.

20 16. The method of claim 15, further comprising:

verifying that said first user has permission to access said first file in response to said first  
access.

25 17. The method of claim 16, wherein said first latency value represents a first time portion  
corresponding to said first access and a second time portion corresponding to said verifying.

18. The method of claim 15, wherein said first user corresponds to a first user type, and wherein said second user corresponds to a second user type.

19. The method of claim 18, further comprising:

creating a first directory for said first user;

populating said first directory with a first plurality of files according to said first user type, wherein said first plurality of files includes said first file;

creating a second directory for said second user; and

populating said second directory with a second plurality of files according to said second user type, wherein said second plurality of files includes said second file.

20. The method of claim 19, further comprising:

wherein said executing said first instance further comprises:

identifying each of said first plurality of files in said first directory; and

creating a first order of said first plurality of files using a first seed value; and

wherein said executing said second instance further comprises:

identifying each of said second plurality of files in said second directory; and

creating a second order of said second plurality of files using a second seed value.

21. The method of claim 15, further comprising:

wherein said logging in said first user further comprises:

logging in said first user using a first operating system protocol; and

wherein said logging in said second user further comprises:

logging in said second user using a second operating system protocol.

22. The method of claim 15, further comprising:

generating a first token in response to said logging in said first user; and

generating a second token in response to said logging in said second user.

23. The method of claim 22, further comprising:

verifying that said first user has permission to access said first file in response to said first access using said first token; and

verifying that said second user has permission to access said second file in response to said second access using said second token.

24. The method of claim 15, wherein said first access comprises a first read access or a first write access, and wherein said second access comprises a second read access or a second write access.

## ABSTRACT OF THE DISCLOSURE

A system and method for testing server latencies using multiple concurrent users in a computer system is provided. A computer system may include a server and one or more clients.

5 Multiple users may be created in the system such that each user may login to the server. The server may include a directory for each user and the directory for each user may be populated with a mix of files according to a user type for each user. An instance of a test program may be executed for each user on one or more clients concurrently. The server may authenticate each user using the same or different operating system protocols. Each instance of the test program  
10 may be configured to cause a series of accesses to one or more files in the directory of its respective user on the server and may be configured to cause a latency value to be measured and stored for each access that is performed. The latency values may be compiled by each instance of the test program and may be stored onto the server upon completion of each instance of the test program. The latency values measured by an instance of the test program may represent a  
15 first time portion that corresponds to the amount of time to perform a given access and a second time portion that corresponds to the server verifying that the user corresponding to this instance of the test program has permission to access the file. The accesses performed may include read accesses or write accesses.



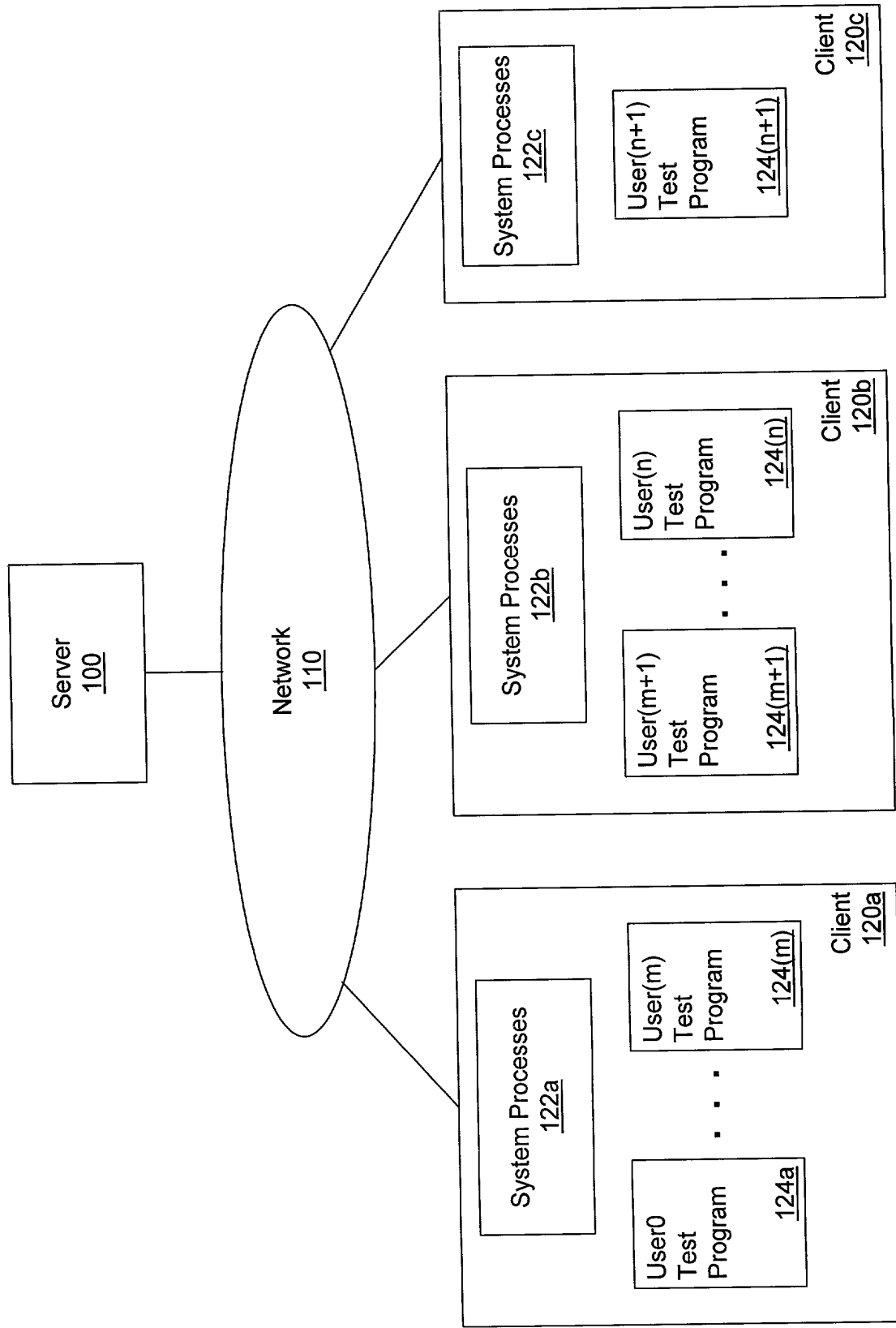


Fig. 1

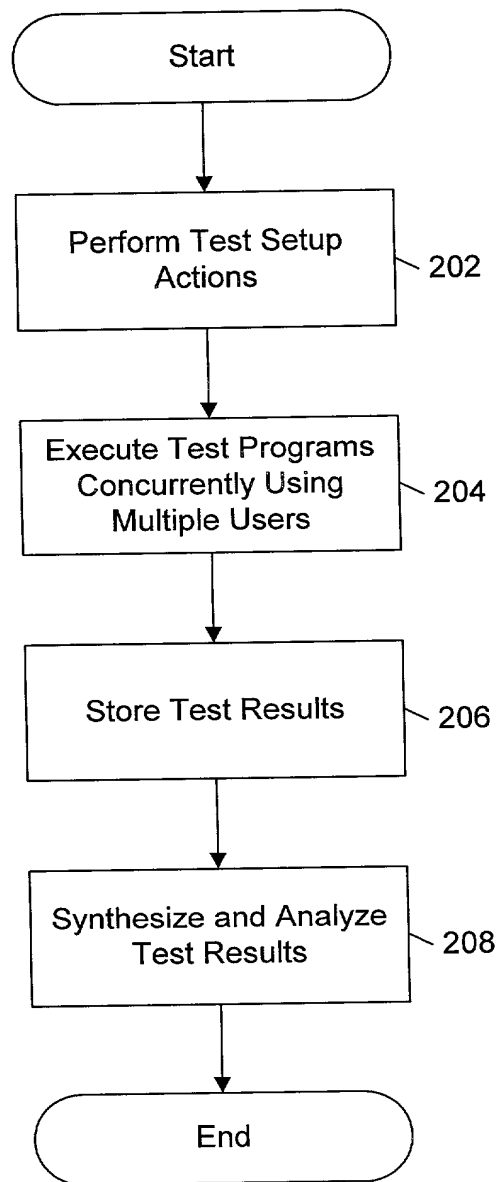


Fig. 2

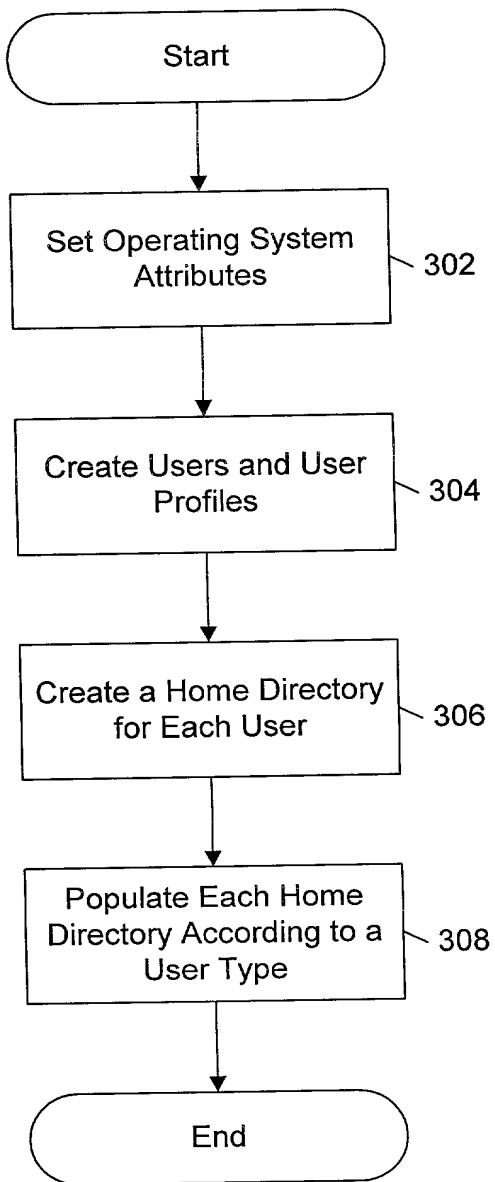


Fig. 3

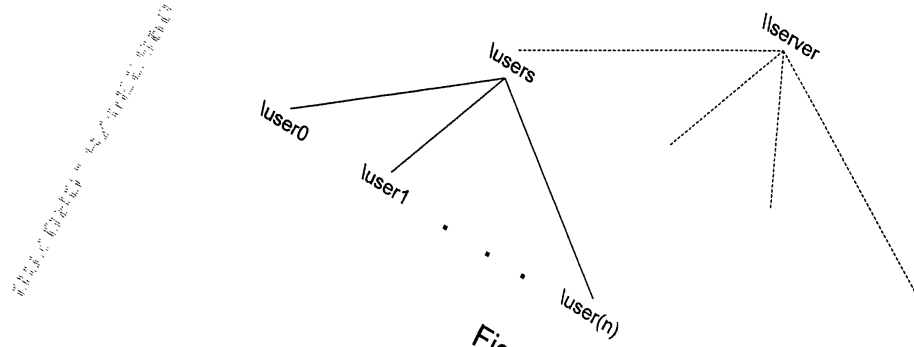


Fig. 4a

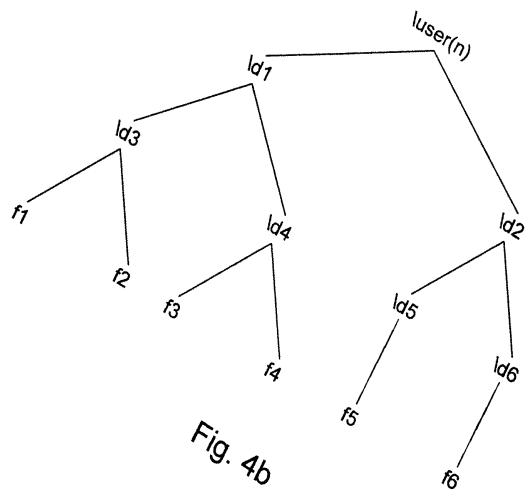


Fig. 4b

User Type	User	File Uses	File Size	Load Rate	Str. Rate	File Load Mix
Small	Clerks	Transaction Records	1 - 2 kilobytes	1 Mb/hr.	6.7 Mb/min.	70% / 20% / 10%
	<ul style="list-style-type: none"> <li>• Sales Assistants</li> <li>• Inventory / Stock Clerks</li> <li>• Accounting Clerks</li> </ul>					
Medium	Managers					
	Secretarial Workers Administrative Workers <ul style="list-style-type: none"> <li>• Human Resource Representatives</li> <li>• Marketing Personnel</li> <li>• Executives</li> </ul>	Memos, Letters	20-80 kilobytes	1.5 Mb/hr.	10 Mb/min.	10% / 70% / 20%
Large	Technical / Creative Workers					
	<ul style="list-style-type: none"> <li>• Engineers</li> <li>• Programmers</li> <li>• Graphic / Mechanical Designers</li> <li>• Architects</li> </ul>	Design Files	0.5 - 2 megabytes	1 Mb/hr.	6.7 Mb/min.	10% / 20% / 70%

Fig. 5

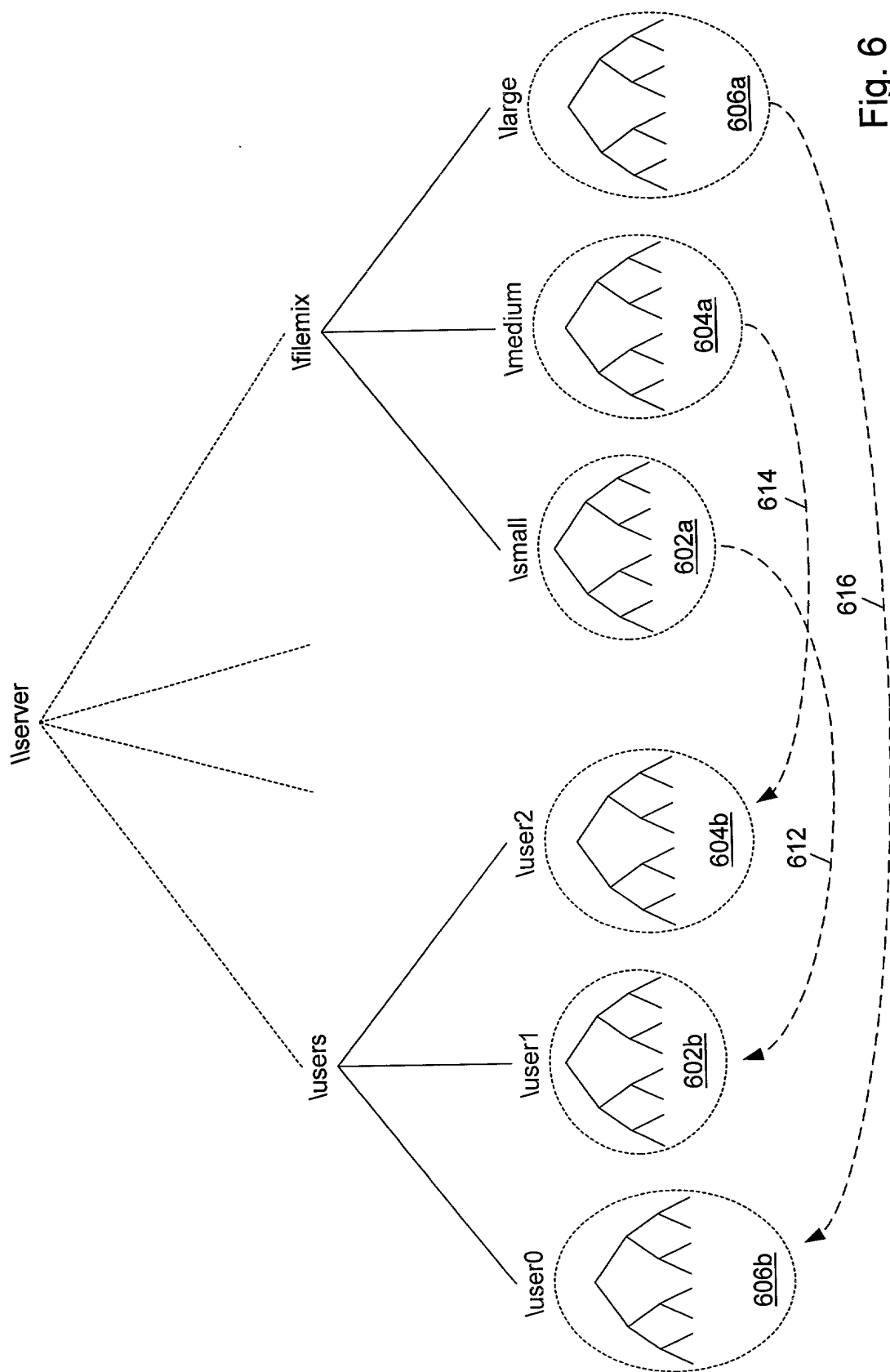


Fig. 6

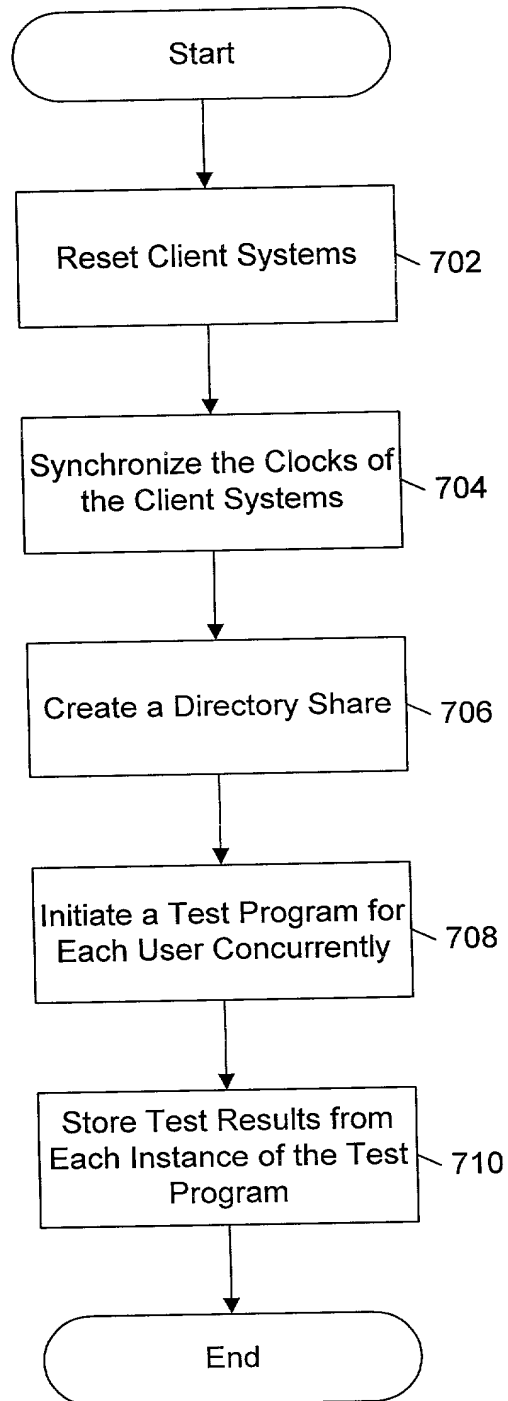


Fig. 7

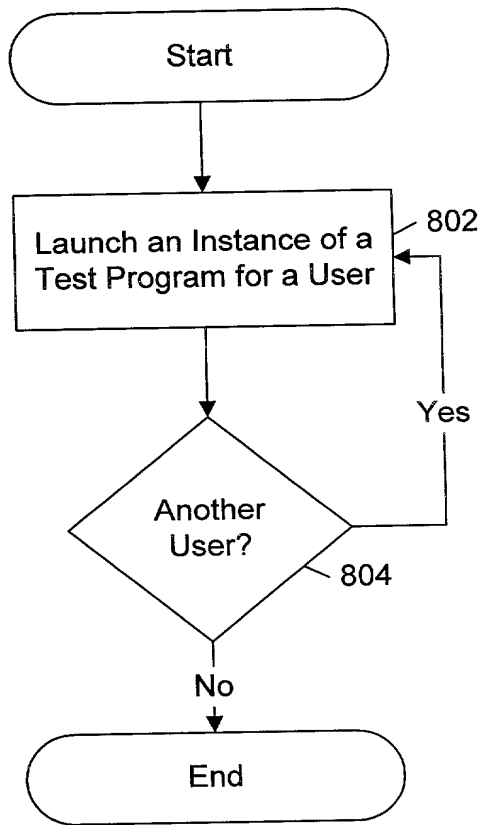


Fig. 8a

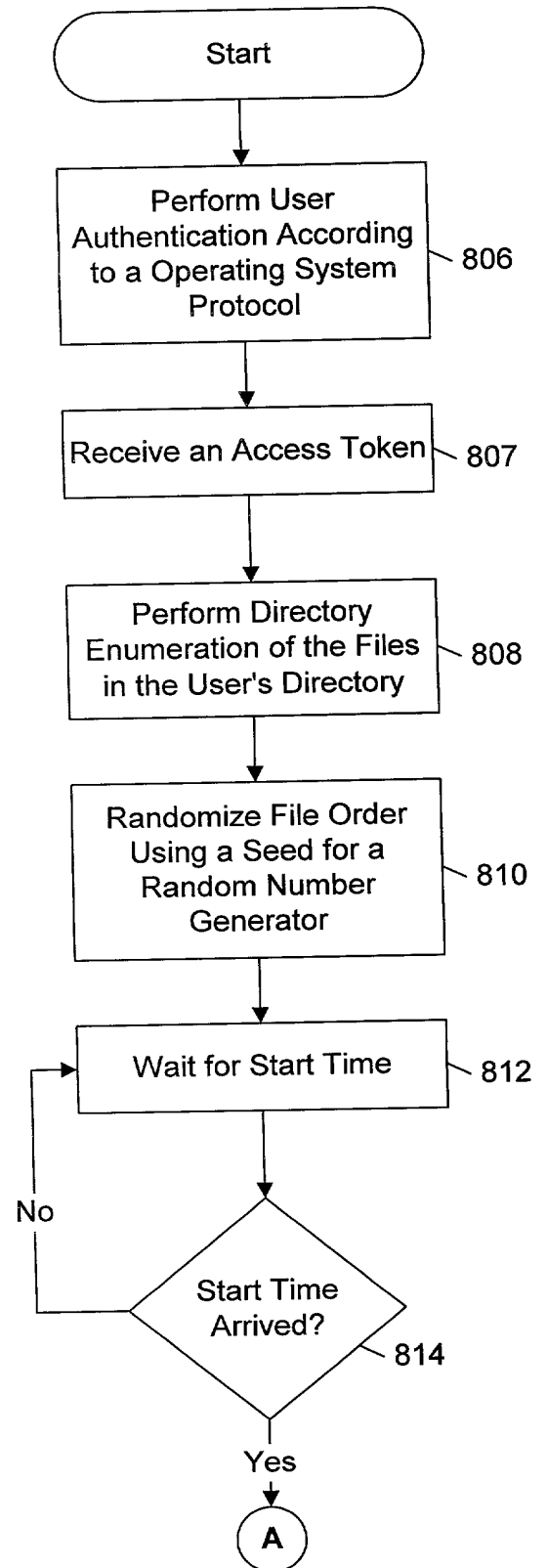


Fig. 8b



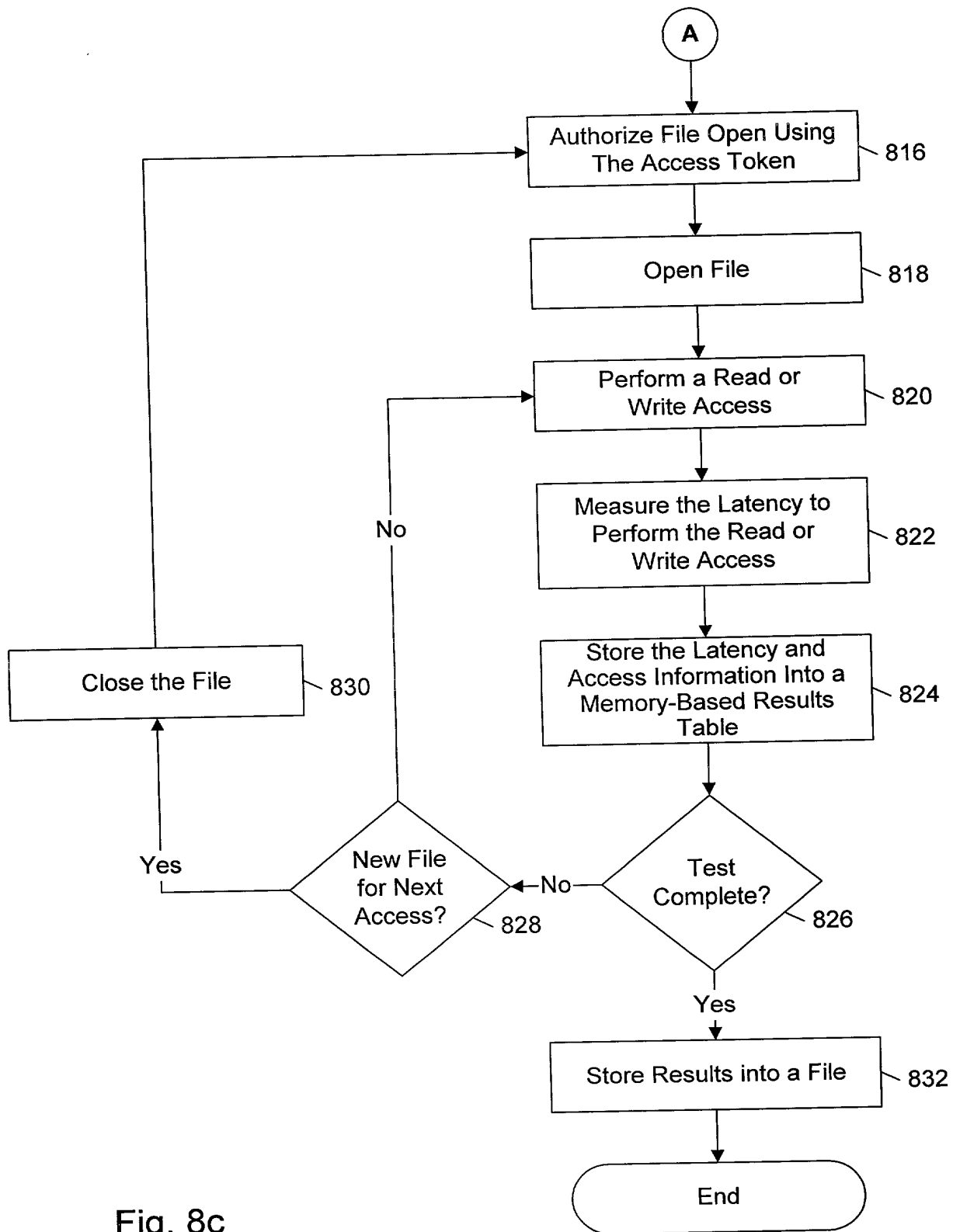


Fig. 8c

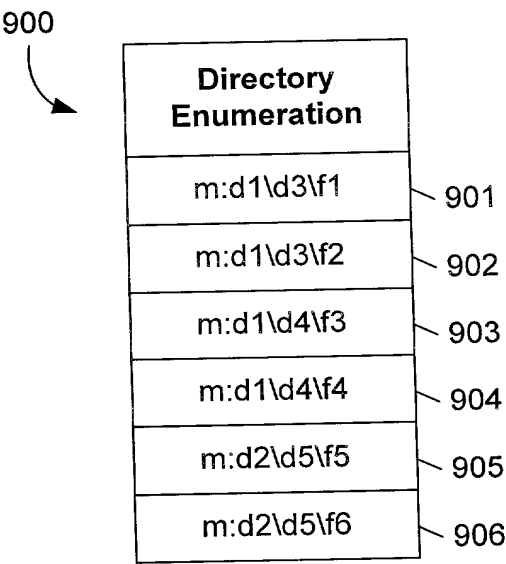


Fig. 9a

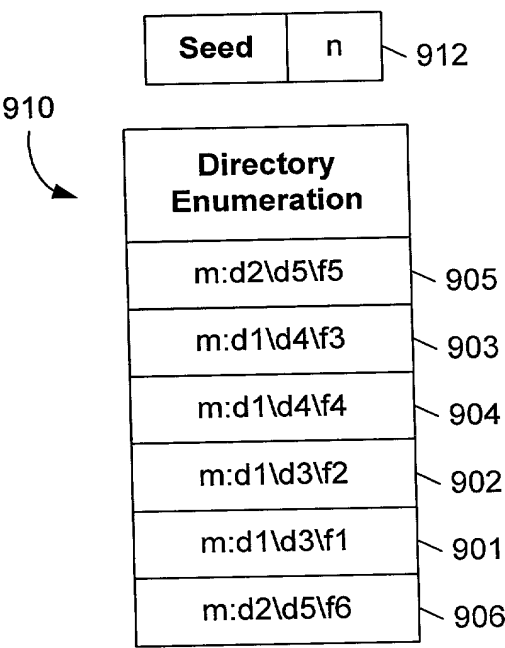


Fig. 9b

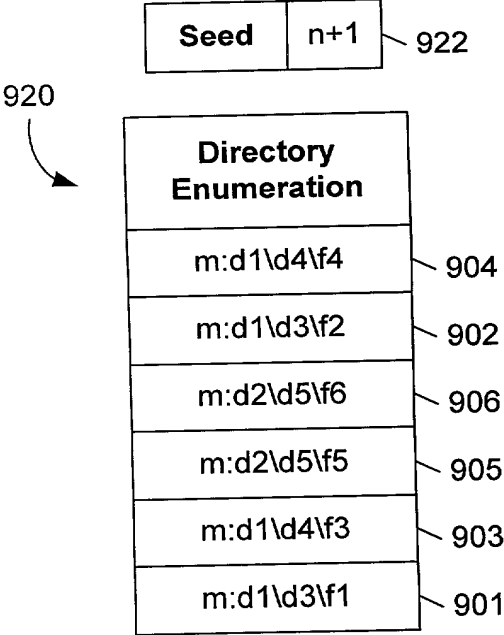


Fig. 9c

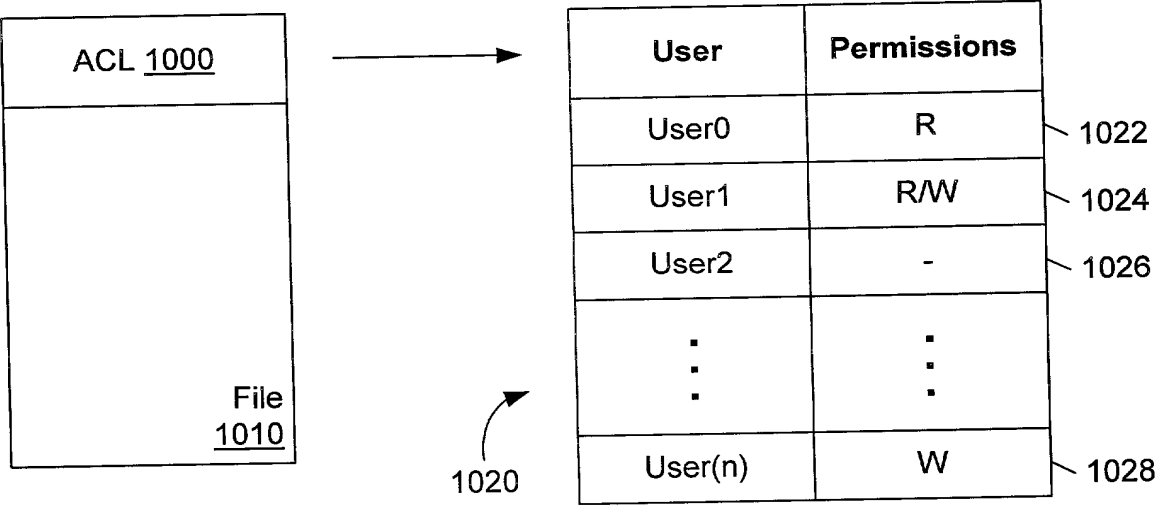


Fig. 10

**DECLARATION AND POWER OF ATTORNEY**

As a below named inventor, I hereby declare that:

My residence, post office address, and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled "**SYSTEM AND METHOD FOR TESTING SERVER LATENCIES USING MULTIPLE CONCURRENT USERS IN A COMPUTER SYSTEM**," the specification of which:

☒ is attached hereto.  
☐ was filed on \_\_\_\_\_ as Application Serial No. \_\_\_\_\_  
and was amended on \_\_\_\_\_ (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose to the Patent and Trademark Office all information known to me to be material to patentability of the subject matter claimed in this application, as "materiality" is defined in 37 C.F.R. § 1.56.

I hereby claim foreign priority benefits under 35 U.S.C. § 119(a)-(d) or § 365(b) of any foreign application(s) for patent or inventor's certificate listed below, or under § 365(a) of any PCT international application listed below designating least one country other than the United States of America, and have identified below any foreign application for patent or inventor's certificate, or of any PCT international application, having a filing date before that of the application on which priority is claimed.

<u>Prior Foreign Application No.</u>	<u>Country</u>	<u>Filing Date</u> <u>(mm/dd/yy)</u>	<u>Priority</u> <u>Claimed</u>	<u>Cert. copy</u> <u>Attached</u>
N/A				

I hereby claim the benefit under 35 U.S.C. § 119(e) of any United States provisional application(s) listed below.

<u>Provisional Application No.</u>	<u>Filing Date</u> <u>(mm/dd/yy)</u>
N/A	

I hereby claim the benefit under 35 U.S.C. § 120 of any United States application(s) listed below, or under § 365(c) of any PCT international application listed below designating the United States of America, and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT international application in the manner provided by the first paragraph of 35 U.S.C. § 112, I acknowledge the duty to disclose all information known to me to be material to the patentability of the subject matter claimed in this application, as "materiality" is defined in 37 C.F.R. § 1.56, which became available between the filing date of the prior application and the national or PCT international filing date of this application.

<u>Parent Application No.</u>	<u>Filing Date</u> <u>(mm/dd/yy)</u>	<u>Parent Patent No. (if applicable) or Status</u>
N/A		

I hereby revoke any previous Powers of Attorney and appoint

Kenneth Olsen	Reg. No. 26,493
Robert S. Hauser	Reg. No. 37,847
Alexander E. Silverman	Reg. No. 37,940
Christine S. Lam	Reg. No. 37,489
Timothy J. Crean	Reg. No. 37,116
Joseph T. FitzGerald	Reg. No. 33,881
Anirma Rakshpal Gupta	Reg. No. 38,275
Sean P. Lewis	Reg. No. 42,798
Michael J. Schallop	Reg. No. 44,319
Bernice B. Chen	Reg. No. 42,403
Kenta Suzue	Reg. No. 45,145
Noreen A. Krall	Reg. No. 39,734
Richard J. Lutton, Jr.	Reg. No. 39,756
Monica D. Lee	Reg. No. 40,696
Marc D. Foodman	Reg. No. 34,110
Naren Chaganti	Reg. No. 44,602

*each of said attorneys being employed by Sun Microsystems; and*

Dan R. Christen	Reg. No. 39,943
Gentry E. Crook	Reg. No. 44,633
Kevin L. Daffer	Reg. No. 34,146
Mark R. DeLuca	Reg. No. 44,649
Jeffrey C. Hood	Reg. No. 35,198
Robert C. Jahnke	Reg. No. 44,800
B. Noël Kivlin	Reg. No. 33,929
Robert C. Kowert	Reg. No. 39,255
Lawrence J. Merkel	Reg. No. 41,191
Eric B. Meyertons	Reg. No. 34,876
Louise K. Miller	Reg. No. 36,609
David W. Quimby	Reg. No. 39,338
David A. Rose	Reg. No. 26,223

*each of said attorneys or agents being a member or an associate of the firm of Conley, Rose & Tayon, P.C., as attorney or agent for so long as they remain with such company or firm, with full power of substitution and revocation, to prosecute the application, to make alterations and amendments therein, to transact all business in the Patent and Trademark Office in connection therewith, and to receive the Letters Patent.*

Please direct all communications to:

B. Noël Kivlin  
Conley, Rose & Tayon, P.C.  
P.O. Box 398  
Austin, Texas 78767-0398  
Phone: (512) 476-1400

I hereby declare that all statements made herein of my own knowledge are true and that all statements made herein on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. § 1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Inventor's Full Name: Mark C. Terranova  
Inventor's Signature: *Mark C. Terranova* Date: 7/20/2000  
City and State (or Foreign Country) of Residence: Maynard, MA Citizenship: U.S.A.  
Post Office and Residence Address: 6 Michael Rd., Maynard, MA 01754  
(Include number, street name, city, state and zip code)

Inventor's Full Name: Michael P. Shea  
Inventor's Signature: *Michael P. Shea* Date: 7/20/2000  
City and State (or Foreign Country) of Residence: Nashua, NH Citizenship: U.S.A.  
Post Office and Residence Address: 10 Winn Road, Nashua, NH 03062  
(Include number, street name, city, state and zip code)

Inventor's Full Name: Robert E. Walsh  
Inventor's Signature: *Robert E. Walsh* Date: 7/22/2000  
City and State (or Foreign Country) of Residence: FOSTER City, CA Citizenship: U.S.A.  
Post Office and Residence Address: 2105 Admiralty Lane, FOSTER City, CA  
(Include number, street name, city, state and zip code) 94404-1629

Inventor's Full Name: Michael V. Iarrobino  
Inventor's Signature: *Michael V. Iarrobino* Date: 7/20/2000  
City and State (or Foreign Country) of Residence: Bedford, NH Citizenship: U.S.A.  
Post Office and Residence Address: 48 Magazine St, Bedford, NH 03110  
(Include number, street name, city, state and zip code)

Post Office and Residence Address: \_\_\_\_\_  
(Include number, street name, city, state and zip code)